

**CLAIMS:**

1. A method of reducing traffic in a decentralised peer-to-peer network, said peer-to-peer network operating over an underlying network comprising first and second network portions, the method comprising:

routing a peer-to-peer message in one of said network portions with an intended destination in the other of said network portions to a gateway between peer-to-peer nodes residing on said first and second network portions; and

controlling transport of said message at said gateway to limit propagation of said message into said other of said network portions.

2. A method as claimed in claim 1 wherein said first network portion comprises a portion of said underlying network managed by a first entity and said second network portion comprises a portion of said underlying network connected to said first network portion across a boundary.

3. A method as claimed in claim 2 implemented to limit a number of peer-to-peer connections across said boundary to a permitted maximum.

4. A method as claimed in claim 1, 2 or 3 wherein said transport controlling comprises blocking said message at said gateway.

5. A method as claimed in claim 1, 2 or 3 wherein said transport controlling comprises redirecting said message to a peer-to-peer node within said one of said network portions.

6. A method as claimed in claim 1, 2 or 3 wherein said transport controlling comprises responding to said message from said gateway.

7. A method as claimed in claim 6 wherein said message comprises a query, and wherein said responding comprises sending a response to said query comprising cached data derived from previous response to queries.
8. A method as claimed in claim 6 wherein said message comprises a file request, and wherein said responding comprises sending a response to said file request comprising previously cached data for a requested file.
9. A method as claimed in claim 1 or 2 wherein said message comprises a file request message, and wherein said controlling comprises modifying a response to a previous file search request such that said response does not indicate that a requested file may be found in said other of said network portions.
10. A method as claimed in claim 9 wherein a said requested file is identified by a hash value.
11. A method as claimed in claim 9 or 10 further comprising storing requested files in a cache, and wherein said response is modified to refer to said cache.
12. A method as claimed in claim 9 or 10 wherein said underlying network comprises a third network portion, and wherein said modifying comprises modifying said response to indicate that said requested file is obtainable from a peer-to-peer node located on said third network portion.
13. A method as claimed in claim 1, 2, 3 wherein said physical network comprises a third network portion, wherein use of each of said network portions has an associated cost, wherein data transport over said third network portion has a cost less than a cost associated with said other of said network portions, and wherein said controlling comprises directing said message into said third network portion.
14. A method as claimed in claim 1 or 2 wherein a said peer-to-peer message has a message identifier, and wherein said controlling comprises:

storing said message identifier for said message,

monitoring message identifiers of messages passing through said gateway, and

limiting propagation of said identified message such that said message passes between said first and second network portions no more than a permitted maximum number of times.

15. A method as claimed in claim 14 wherein said permitted maximum number of times is one.

16. A method as claimed in any preceding claim wherein said network portions comprise domains of an internet.

17. A method as claimed in any preceding claim wherein said one of said network portions comprises said first network portion and said other of said network portions comprises said second network portion.

18. A computer network message controller for reducing traffic in a decentralised peer-to-peer network, said peer-to-peer network operating over a physical network comprising first and second network portions, said network message controller comprising:

a router for routing a peer-to-peer message in one of said first network portions with an intended destination in the other of said network portions to a gateway between peer-to-peer nodes residing on said first and second network portions; and

a gateway controller configured to control transport of said message into said other of said network portions

19. A computer network message controller as claimed in claim 18 wherein said first network portion comprises a portion of said physical network managed by a first

entity and said second network portion comprises a portion of said physical network connected to said first network portion across a boundary.

20. A computer network message controller as claimed in claim 19 wherein said gateway controller is configured to wherein said gateway controller is configured to limit a number of peer-to-peer connections across said boundary to a permitted maximum.

21. A computer network message controller as claimed in claim 18, 19 or 20 wherein said gateway controller is configured to block said message at said gateway.

22. A computer network message controller as claimed in claim 18, 19 or 20 wherein said gateway controller is configured to redirect said message to a peer-to-peer node within said one of said network portions.

23. A computer network message controller as claimed in claim 18, 19 or 20 wherein said gateway controller is configured to respond to said message.

24. A computer network message controller as claimed in claim 23 further comprising a cache to store data, wherein said message comprises a query, and wherein said gateway controller is configured to send a response to said query including data from said cache.

25. A computer network message controller as claimed in claim 23 wherein said message comprises a file request, further comprising a cache to store data derived from previous responses to file requests, and wherein said gateway controller is configured to send a response to said file request including data from said cache.

26. A computer network message controller as claimed in claim 18 or 19 wherein said message comprises a file request message, and wherein said gateway controller is configured to modify a response to a previous file search request such that said response does not indicate that a requested file may be found in said other of said network portions.

27. A computer network message controller as claimed in claim 26 wherein a said requested file is identified by a hash value.

28. A computer network message as claimed in claim 26 or 27 further comprising a cache for storing requested files, and where said gateway controller is configured to modify said response to refer to said cache.

29. A computer network message as claimed in claim 18, 19 or 20 wherein said underlying network comprises a third network portion, and wherein said gateway controller is configured to modify said response to indicate that said requested file is obtainable from a peer-to-peer node located on said third network portion.

30. A computer network message controller as claimed in claim 18 or 19 wherein a said peer-to-peer message has a message identifier, and wherein said gateway controller is configured to store said message identifier for said message, monitor message identifiers of messages passing through said gateway, and limit propagation of said identified message such that said message passes between said first and second network portions no more than a permitted maximum number of times.

31. A computer network message controller as claimed in claim 30 wherein said permitted maximum number of times is one.

32. A computer network message controller as claimed in any one of claims 18 to 31 wherein said one of said network portion comprises said first network portion and said other of said network portions and said other of said network portions comprises said second network portion, and wherein said router and said gateway controller comprise part of said first network portion.

33. A computer network message controller as claimed in any one of claim 18 to 32 wherein said one of said network portions comprises said first network portion and said other of said network portions comprises said second network portion.

34. A computer network message controller as claimed in any one of claims 18 to 33 wherein said gateway controller comprises a processor, and program memory storing processor control code coupled to said processor to load and implement said code, said code comprising code to configure said gateway controller to operate as claimed in any one of claims 18 to 33.

35. A carrier carrying the processor control code of claim 34.

36. A gateway controller, in particular for the computer network message controller of claim 18, for reducing traffic in a decentralised peer-to-peer network operating over an underlying network comprising first and second network portions, the controller being configured for operation at a gateway between peer-to-peer nodes residing on said first and second network portions, the gateway controller comprising:

an interface for said first and second network portions, for receiving a peer-to-peer message in one of said first network portions with an intended destination in the other of said network portions; and

a controller configured to control transport of said message into said other of said network portions.

37. A gateway controller as claimed in claim 36 wherein said controller is configured to block said message at said gateway.

38. A gateway controller as claimed in claim 36 or 37 wherein said controller is further configured to redirect a said message to a peer-to-peer node within said one of said network portions.

39. A gateway controller as claimed in claim 36, 37 to 38 wherein said controller is further configured to respond to a said message.

40. A gateway controller as claimed in claim 39 comprising a query cache to store data derived from responses to queries, and wherein said controller is configured to respond to a said query using data from said query cache.

41. A gateway controller as claimed in claim 39 or 40 further comprising a file request cache to store data derived from responses to file requests, and wherein said controller is configured to respond to a said file request using data from said file request cache.

42. A gateway controller as claimed in any one of the claims 36 to 41 wherein said first and second network portions comprise physical portions of said underlying network.

43. A gateway controller as claimed in claim 36 wherein said message comprises a file request message, and wherein said controller is configured to modify a response to a previous file search request such that said response does not indicate that a requested file may be found in said other of said network portions.

44. A gateway controller as claimed in claim 43 wherein a said requested file is identified by a hash value.

45. A gateway controller as claimed in claim 43 or 44 further comprising a cache for storing requested files, and wherein said controller is configured to modify said response to refer to said cache.

46. A gateway controller as claimed in claim 36 wherein said underlying network comprises a third network portion, and wherein said controller is configured to modify said response to indicate said requested file is obtainable from a peer-to-peer node located on said third network portion.

47. A gateway controller as claimed in claim 36 wherein a said peer-to-peer message has a message identifier, and wherein said controller is configured to store said message identifier for said message, monitor message identifiers of messages passing

through said gateway, and limit propagation of said identified message such that said message passes between said first and second network portions no more than a permitted maximum number of times.

48. A gateway controller as claimed in claim 47 wherein said permitted maximum number of times is one.

49. A gateway controller as claimed in claim 36 wherein said first network portion comprises a portion of said underlying network managed by a first entity and said second network portion comprises a portion of said underlying network connected to said first network portion across a boundary, and wherein said controller is configured to provide a limited number of peer-to-peer connections across said boundary.

50. A gateway controller as claimed in any one of claims 36 to 49 wherein said one of said network portions comprises said first network portion and said other of said network portions comprises said second network portion.

51. A gateway controller as claimed in any one of claims 36 to 50 wherein said network portions comprise domains of an internet.

52. A gateway controller as claimed in any one of claims 36 to 51 wherein said controller comprises a processor, and program memory storing processor control code coupled to said processor to load and implement said code, said code comprising code to configure said controller to control transport of said message into said other of said network portions.

53. A carrier carrying the processor control code of claim 52.

54. A peer-to-peer network cache comprising:

a network interface for interfacing to a network over which said peer-to-peer network operates;



35

a data store for storing cached data files each in association with a data file identifier, a data file identifier comprising a value computed from the contents of a data file it identifies;

program memory storing processor control code; and

a processor coupled to said network interface, to said data store, and to said program memory for implementing said processor control code, said code comprising code for controlling the processor to:

read peer-to-peer traffic on said network;

identify a request for a data file within said peer-to-peer traffic:

identify the requested data file from a said data file identifier within said peer-to-peer traffic; and

provide said requested data file from said data store to a peer-to-peer node making said request.

55. A peer-to-peer network cache as claimed in claim 53 wherein said request includes said data file identifier.

56. A peer-to-peer network cache as claimed in claim 53 wherein said data file identifier is provided by a peer-to-peer node responding to said request.

57. A peer-to-peer network cache as claimed in claim 54, 55 or 56 wherein said code further comprises code to:

identify a response to said request within said peer-to-peer traffic; and

modify said response to address a data file within said data store.

58. A peer-to-peer network cache as claimed in any one of claims 54 to 57 wherein said cache comprises an active node of said peer-to-peer network.

59. A peer-to-peer network cache as claimed in any one of claims 54 to 58 wherein said code further comprises code to:

obtain said requested data file from said peer-to-peer network; and

store said requested data file in said data store.

60. A peer-to-peer network cache as claimed in claim 59 wherein said code further comprises code to:

identify duplicate data files using said data file identifiers; and

limit the number of duplicate data files stored in said data store.

61. A peer-to-peer network cache as claimed in any one of claims 54 to 60 wherein said data file identifier comprises a has or checksum function.

62. A peer-to-peer network cache as claimed in any one of claims 54 to 61 wherein said peer-to-peer network comprises a decentralised peer-to-peer network.

63. A carrier carrying the processor control code of any one of claims 54 to 62.

64. A method of reducing traffic in a distributed peer-to-peer network, the method comprising:

monitoring peer-to-peer traffic of said network;

identifying a request for a data file within said peer-to-peer traffic;

identifying the requested data file from a data file identifier associated with said request within said peer-to-peer traffic; and

providing said requested data file from a cache to a peer-to-peer node making said request.

65. Computer program code to, when running, implement the method of claim 64.

66. A carrier carrying the computer program code of claim 65.

67. A peer-to-peer network cache for modifying peer-to-peer network traffic, the network cache comprising:

a network interface for interfacing to a network over which said peer-to-peer network operates;

a data store for storing digital fingerprint data for identifying data files, and corresponding data file source identifiers; and

program memory storing processor control code; and

a processor coupled to said network interface, to said data store and to said program memory for implementing said processor control code, said code comprising code for controlling the processor to:

reads peer-to-peer traffic on said networks;

identify a response to a peer-to-peer file request within said peer-to-peer traffic, said response including a digital fingerprint of a requested file;

identify from said data store an alternative source for said requested file to a source of said response; and

reply to said file request using said alternative source.

68. A peer-to-peer network cache as claimed in claim 67 wherein said data store is further configured for storing said data file, and wherein said code further comprises code to modify said response to index a requested data file stored in said data store.

69. A peer-to-peer network cache as claimed in claim 67 or 68 wherein said code further comprises code to:

read said peer-to-peer traffic to identify digital fingerprint data and corresponding source identification data for data files; and

store said digital fingerprint data and source identification data in said data store.

70. A peer-to-peer network cache as claimed in claim 69 wherein said code further comprises code to:

read said peer-to-peer data file data; and

store said data file data in association with digital fingerprint data for said data file data in said data store.

71. A peer-to-peer network cache as claimed in any one of claims 67 to 70 wherein said digital fingerprint data comprises hash value data.

72. A carrier carrying the processor control code of any one of claims 67 to 71.

73. A method of modifying peer-to-peer network traffic in a distributed peer-to-peer network, the method comprising:

reading peer-to-peer traffic on said network;

identifying a response to a peer-to-peer file request within said peer-to-peer traffic, said response including a digital fingerprint of a requested file;

identifying from a cache an alternative source for said requested file to a source of said response; and

replying to said file request using said alternative source.

74. A carrier carrying computer program code to, when running, modifying peer-to-peer network traffic in a distributed peer-to-peer network, by:

reading peer-to-peer traffic on said network;

identifying a response to a peer-to-peer file request within said peer-to-peer traffic, said response including a digital fingerprint of a requested file;

identifying from a cache an alternative source for said requested file to a source of said response; and

replying to said file request using said alternative source.